Hi, I'm Mike Chapple and this is the audio review of the study essentials for chapter 17 of the official CISSP study guide. Here are the top things that you need to know from this chapter on preventing and responding to incidents. List and describe the incident management steps. The CISSP security operations domain lists incident management steps such as detection, response, mitigation, reporting, recovery, remediation and lessons learned. After detecting and verifying an incident, the first response is to limit or contain the scope of the incident while protecting evidence. Based on governing laws, an organization may need to report an incident to official authorities and if PII is effective, individuals need to be informed. The remediation and lessons learned stages include root cause analysis to determine the cause and recommend solutions to prevent a recurrence.

Understand basic preventive measures. Basic preventive measures can prevent many incidents from occurring. These include keeping systems up to date, removing or disabling unneeded protocols and services, using intrusion detection and prevention systems, using anti-malware software with up to date signatures and enabling both host-based and network-based firewalls. Know the difference between whitelisting and blacklisting. Software whitelists provide a list of approved software and prevent the installation of any other software not on the list. Blacklists provide a list of unapproved software and prevent the installation of any software on the list.

Understand sandboxing. Sandboxing provides an isolated environment and prevents code running in a sandbox from interacting with elements outside of the sandbox. Know about third party provided security services. Third-party security services help an organization augment security services provided by internal employees. Many organizations use cloud-based solutions to augment their internal security.

Know about denial-of-service DoS attacks. DoS attacks prevent a system from responding to legitimate requests for service. A common DoS attack is the SYN flood attack, which disrupts the TCP three-way handshake. Even though older attacks are not as common today, because basic precautions block them, you may still be tested on them, because many newer attacks are variations on older methods. Smurf attacks employ an amplification network to send numerous response packets to a victim, ping of death attack send numerous oversized ping packets to the victim causing the victim's system to freeze, crash or reboot.

Understand zero-day exploits. A zero-day exploit is an attack that uses a vulnerability that's either unknown to anyone but the attacker or known only to a limited group of people. On the surface, it sounds like you can't protect against an unknown vulnerability, but basic security practices go a long way toward preventing zero-day exploits. Removing or disabling unneeded protocols and services reduces the attack surface, enabling firewalls, blocks many access points and using intrusion detection and prevention systems helps detect and block potential attacks. Additionally, using tools such as honeypots help protect live networks.

Understand man-in-the-middle attacks. A man-in-the-middle attack sometimes called an on-path attack occurs when a malicious user is able to gain a logical position between the two endpoints of a communications link. Although it takes a significant amount of sophistication on the part of an attacker to complete a man-in-the-middle attack, the amount of data obtained from the attack can be significant.

Understand intrusion detection and intrusion prevention. IDSs and IPSs are important detection and prevention measures against attacks. Know the difference between knowledge-based detection using a database similar to anti-malware signatures and behavior-based detection. Behavior-based detection starts with a baseline to recognize normal behavior and compares activity with a baseline to detect abnormal activity. The baseline can be outdated if the network is modified, so it must be updated when the environment changes.

Describe honeypots and honeynets. A honeypot is a system that typically has pseudo flaws and fake data to lure intruders. A honeynet is two or more honeypots in a network. Administrators can observe attacker activity while they're in the honeypot, and as long as attackers are in the honeypot, they're not on the live network.

Understand the methods used to block malicious code. Malicious code can be thwarted with a combination of tools. The obvious tool is anti-malware software with up-to-date definitions installed on each system at the boundary of the network and on email servers. However, policies that enforce basic security principles such as the least privileged principle prevent regular users from installing potentially malicious software. Additionally, educating users about the risks and the method attackers commonly use to spread viruses helps users understand and avoid dangerous behaviors.

Know the types of log files. Log data is recorded in databases and different types of log files. Common log files include security logs, system logs, application logs, firewall logs, proxy logs and change management logs. Log files should be protected by centrally storing them and using permissions to restrict access, archive logs should be set to read only to prevent modification.

Monitoring is a form of auditing that focuses on active review of log file data. Monitoring is used to hold subjects accountable for their actions and to detect abnormal or malicious activities. It is also used to monitor system performance. Monitoring tools such as IDSs or SIEMs automate continuous monitoring and provide real-time analysis of events, including monitoring what happens inside a network, traffic entering a network, and traffic leaving a network also known as Egress monitoring.

Log management includes analyzing logs and archiving logs. Be able to explain audit trails. Audit trails are the records created by recording information about events and occurrences into one or more databases or log files. They're used to reconstruct an event, extract information about an incident and prove or disprove culpability. Using audit trails as a passive form of a detective security control and audit trails are essential evidence in a criminal prosecution.

Understand how to maintain accountability. Accountability is maintained for individual subjects through the use of auditing. Logs record user activity and users can be held accountable for their logged actions. This directly promotes good user behavior and compliance with the organization's security policy.

Describe threat feeds and threat hunting. Threat feeds provide organizations with a steady stream of raw data. By analyzing threat feeds, security administrators can learn of current threats. They can then use this knowledge to search through the network looking for signs of these threats.